

UNDER SEAL

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

One black Samsung Galaxy S9 (SM-G960UZZKATMB
64GB 18.03, IMEI: 353309/09/151908/0,
S/N: R28K31M3BWJ)

Case No. 1:19-SW-194

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

One black Samsung Galaxy S9 (SM-G960UZZKATMB 64GB 18.03, IMEI: 353309/09/151908/0, S/N: R28K31M3BWJ), as described in Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841(a)(1) & 846	Conspiracy to distribute a controlled substance.

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SAUSA Lynda Lao/AUSA James Trump

Applicant's signature

Michael Jeng, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

MARCH 14, 2019

/s/ JFA
John F. Anderson
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is a black Samsung Galaxy S9 (SM- G960UZZKATMB 64 GB 18.03, IMEI: 353309/09/151908/0, S/N: R28K31M3BWJ). The Device is currently located in an FBI evidence locker at 9325 Discovery Boulevard, Manassas, Virginia.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device, described in Attachment A, that relate to violations of the Federal Criminal Code involving controlled substances and Spencer Pak, including:
 - a. any conversations, whether through text messages or other applications, where Spencer Pak discusses marijuana or any other controlled substance;
 - b. lists of customers and related identifying information;
 - c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - e. any information recording the schedules of Spencer Pak to the date the Device came into law enforcement possession;
 - f. any photographs of controlled substances;
 - g. all bank records, checks, credit card bills, account information, and other financial records;
 - h. records of Internet Protocol addresses used; and
 - i. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

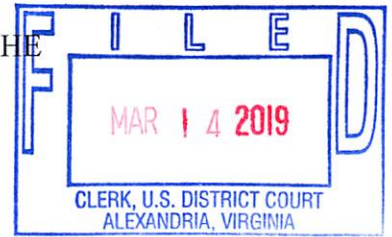
As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF

One black Samsung Galaxy S9 (SM-
G960UZZKATMB 64GB 18.03, IMEI:
353309/09/151908/0, S/N: R28K31M3BWJ)

CURRENTLY LOCATED AT
FBI EVIDENCE LOCKER
9325 Discovery Boulevard
Manassas, VA 20109

UNDER SEAL

Case No. 1:19-SW-194

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT**

1. I, Michael Jeng, Special Agent of the Federal Bureau of Investigation (FBI), Washington (D.C.) Field Office (WFO), Northern Virginia Resident Agency (NVRA), being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— one (1) black Samsung Galaxy S9 (SM- G960UZZKATMB 64 GB 18.03, IMEI: 353309/09/151908/0, S/N: R28K31M3BWJ —which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

3. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code. I am also a “federal law enforcement officer” within the meaning of Rule 41 of the Federal Rules of Criminal Procedure and authorized to request a federal search warrant.

4. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since June 2017. In that time, I have been a member of a transnational organized crime squad. My primary duties include the enforcement of federal laws related to crimes committed by transnational organizations and criminal street gangs. As a Special Agent, I have participated in controlled purchases of illegal narcotics, conducted visual and electronic surveillance, executed arrest, search, and seizure warrants, and interviewed many individuals involved in drug trafficking and gang activities. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology of drug traffickers.

5. I know that it is common for individuals engaged in the distribution of controlled substances to use telephonic communications, both cellular (to include voice and text messages) and hard line, to further their criminal activities by coordinating the distribution of narcotics, illegal proceeds of narcotics trafficking, and other efforts of co-conspirators. I know that individuals engaging in the distribution of controlled substances use cellular telephones to exchange information with customers and/or source(s) of supply through text messaging, instant messaging, and in direct telephone conversations.

6. I know that it is common for narcotics traffickers to utilize multiple mobile telephones to communicate with co-conspirators in order to compartmentalize their illegal activity and avoid detection by law enforcement. Additionally, I am aware that narcotics traffickers utilize fictitious names, vehicles, and real property to circumvent law enforcement. I know that "smart" phones play an integral role in the daily lives of individuals engaging in the distribution of controlled substances and that these individuals use cellular telephones to exchange information with customers and/or source(s) of supply through text messaging, instant messaging, and telephone conversations.

7. The facts and information contained in this affidavit are based upon my personal knowledge, information obtained from federal, state and local law enforcement officers, and information obtained from interviews and analysis of reports.

PROBABLE CAUSE

8. Spencer Pak (Pak) is a member of the Reccless Tigers (Tigers), a criminal street gang operating in Northern Virginia. Special Agents from the FBI's WFO have interviewed over two dozen individuals who are members or associates of the Tigers. Approximately ten of these individuals have identified Pak as a member of the Tigers. The FBI knows that narcotic trafficking, including marijuana and cocaine, is a major source of revenue for the Tigers.

9. On February 15, 2019, an arrest warrant was issued for Pak based on a criminal complaint filed in Case No. 1:19-mj-90. Pak and three others were charged with conspiracy to distribute cocaine in violation of Title 21, United States Code, Sections 841 and 846. These charges were based on a series of undercover drug purchases made by a confidential informant (CI) working with law enforcement and an undercover law enforcement officer, or undercover employee (UCE), from on or about August 2017 to on or about September 2018. The CI conducted three drug buys from Pak and his co-conspirators while the UCE conducted eight. In total, Pak and his co-conspirators sold the CI and UCE approximately 713.98 grams of cocaine.

10. During these undercover drug purchases, Pak relied upon the calling and texting capabilities of his cellphone to coordinate drug sales. Prior to every drug deal they made, the UCE and Pak would coordinate via cellphone calls and texts regarding details of the sale such as meeting place, time, quantity of drugs, and cost. For example, on May 31, 2018, Pak sent the UCE a text message setting the time and location of the drug deal, asking if the "same spot cool." In some instances, Pak used cellphone communications to inform the UCE of whether Pak or one of his co-conspirators would conduct the sale. For example, on August 21, 2018, Pak sent the UCE a text message stating that Pak's "homegirl" would be there in a "black or gray Mercedes." Later on

that day, the UCE did indeed conduct the drug purchase with a female who drove a Mercedes instead of with Pak. Finally, when Pak changed his phone number, he informed the UCE via a text message on August 20, 2018 which suggested that he (Pak) just got a new phone and that he (Pak) was “Sean the pizza guys.”¹ All of these are examples of how Pak relied upon his cellphone to conduct his drug sales.

11. Pak was arrested on February 16, 2019 pursuant to an arrest warrant, when the Loudoun County’s Sheriff Office (LCSO) conducted a traffic stop on a vehicle that Pak was driving. Upon approaching the vehicle, LCSO officers detected a strong odor of marijuana coming from inside the vehicle and observed in plain view two cigars with green leafy plant material inside their wrappers. Additional green leafy substances were found on the person of the passenger, identified as Richard Pak (Richard). The green leafy substances were later field tested and confirmed to be marijuana. Also, a loaded Glock handgun was found concealed in the glove compartment. Pak also had a black Samsung Galaxy S9 (SM- G960UZKATMB 64 GB 18.03, IMEI: 353309/09/151908/0, S/N: R28K31M3BWJ). This cellphone was seized by law enforcement and is the subject of this search warrant.

12. The cellular phone is currently in the lawful possession of the FBI. The cellular phone—one (1) black Samsung Galaxy S9 (SM- G960UZKATMB 64 GB 18.03, IMEI: 353309/09/151908/0, S/N: R28K31M3BWJ)—was seized from Pak by LCSO incident to Pak’s arrest on February 16, 2019. Therefore, while law enforcement authorities might already have all necessary authority to examine the cellular phone, I seek this additional warrant out of an abundance of caution to be certain that an examination of the cell phone will comply with the Fourth Amendment and other applicable laws.

¹ Based on our investigation, we are aware that Pak uses the word “pizza” as a code word for cocaine.

13. The cellular phone is currently in storage at 9325 Discovery Boulevard, Manassas, VA 20109. In my training and experience, I know that the cellular phone has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when it first came into the possession of the Federal Bureau of Investigations.

14. Based on the foregoing, I submit there is probable cause to believe that evidence of Pak's drug trafficking activities in violation of Title 21, United States Code, Sections 841 and 846, will be found on the cell phone that is the subject of this search warrant.

TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. *Digital camera*: A digital camera is a camera that records pictures as digital picture

files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. *Portable media player*: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly

available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.
- f. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <https://www.apple.com/iphone/>, I know that the cellular phone could have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the

device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement’s possession, the execution of this warrant does not involve the

physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

ATTACHMENTS

21. In addition to Attachments A and B described above, attached to this affidavit as Attachment C is the February 15, 2019, complaint affidavit in Case No. 1:19-mj-90.

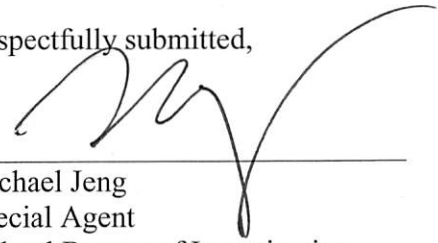
CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B. I declare under penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.

REQUEST FOR SEALING

23. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Michael Jeng
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 14th day of March 2019.

 /s/ JFA
John F. Anderson
United States Magistrate Judge
The Honorable John F. Anderson
United States Magistrate Judge
Alexandria, Virginia

ATTACHMENT A

The property to be searched is a black Samsung Galaxy S9 (SM- G960UZZKATMB 64 GB 18.03, IMEI: 353309/09/151908/0, S/N: R28K31M3BWJ). The Device is currently located in an FBI evidence locker at 9325 Discovery Boulevard, Manassas, Virginia.

• This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device, described in Attachment A, that relate to violations of the Federal Criminal Code involving controlled substances and Spencer Pak, including:
 - a. any conversations, whether through text messages or other applications, where Spencer Pak discusses marijuana or any other controlled substance;
 - b. lists of customers and related identifying information;
 - c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - e. any information recording the schedules of Spencer Pak to the date the Device came into law enforcement possession;
 - f. any photographs of controlled substances;
 - g. all bank records, checks, credit card bills, account information, and other financial records;
 - h. records of Internet Protocol addresses used; and
 - i. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.